ANALYSABLE CHAOS-BASED DESIGN PARADIGMS FOR CRYPTOGRAPHIC APPLICATIONS

ABUBAKAR ABBA

UNIVERSITI SAINS MALAYSIA

2024

ANALYSABLE CHAOS-BASED DESIGN PARADIGMS FOR CRYPTOGRAPHIC APPLICATIONS

by

ABUBAKAR ABBA

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

July 2024

ACKNOWLEDGEMENT

First and foremost, I would like to express my heartfelt gratitude to God, ALLAH, for providing me with the strength and courage to undertake and complete this work. I am deeply grateful to my wife, Amina H. Aliyu, for her support and understanding throughout the years of my PhD research. Her patience and encouragement were invaluable in making this journey possible. Not forgetting my parents, especially my compassionate mother, Haj Amina Jafaru Aliyu, who has been my pillar of support throughout this challenging journey. Also, want to express my appreciation to my Guardian, Alh Sani Abba, whose guidance and support have played an invaluable role in shaping my path and achievements. Their encouragement and love have been instrumental in my success during this grueling process.

Next, I would like to express my esteemed thanks and appreciation to my supervisors, Dr. Teh Je Sen, and Dr. Mohd Najwadi Yusoff, for their patience, continuous support, ideas and motivation throughout my entire study, they have been a constant source of inspiration and introduced me to the field of cryptography. They are very dedicated supervisors, willing to do anything to help their students. Words alone cannot fully express the depth of my appreciation and respect for them. I would also like to thank Prof. Dr. Rosni Abdallah and Dr. Moatsum for their words of advice, support and encouragement.

Last but not the least, I would like to thank Universiti Sains Malaysia for providing the necessary educational facilities that played a role in the success of this thesis. I am also deeply thankful to the Nigerian Tertiary Education Trust Fund for supporting my research through MyPhD scholarship, which has enabled me to pursue and complete my research.

TABLE OF CONTENTS

ACKNOWLEDGEMENT ..... **ii**

TABLE OF CONTENTS ..... **iii**

LIST OF TABLES ..... **viii**

LIST OF FIGURES ..... **x**

LIST OF ABBREVIATIONS ..... **xii**

LIST OF APPENDICES ..... **xiv**

ABSTRAK ..... **xv**

ABSTRACT ..... **xvii**

CHAPTER 1 INTRODUCTION **1**

1.1 Background 1

1.2 Problem Statement 3

1.3 Research Motivation 6

1.4 Research Objectives 7

1.5 Research Contributions 8

1.6 Scope of the Research 9

1.7 Research Methodology 10

1.8 Organization of Thesis 13

CHAPTER 2 LITERATURE REVIEW **14**

2.1 Introduction 14

2.2 Design Paradigms 15

2.2.1 Substitution-Permutation Network (SPN) 16

2.2.2 Feistel Network 17

2.2.3 ARX Structure 18

2.2.4 Sponge Construction 19

2.2.5 Davis Meyer Construction 20

2.3 Chaos Theory and Cryptography 21
2.4 Chaotic Maps 24
2.4.1 1 Dimensional Chaotic Map 25
2.4.2 HD Chaotic Maps 28
2.4.3 Chaotic Maps as a Dynamic System 30
2.5 Chaos Quantification 31
2.5.1 Bifurcation Diagram 32
2.5.2 Lyapunov Exponent 33
2.5.3 Histogram 34
2.5.4 Shannon Entropy 35
2.6 Chaos-Based Cryptographic Applications 36
2.6.1 Image Encryption 36
2.6.2 Hash Function 39
2.7 Research Gap and Discussion 42
2.8 Summary 46
CHAPTER 3 METHODOLOGY 47
3.1 Introduction 47
3.2 The General Framework 47
3.3 Analysis of Keyspace of Existing Chaos-Based Primitives 50
3.4 The New Key Schedule 50
3.5 Analysis and Construction of New Design Paradigms 52
3.6 New Image Encryption Algorithm 54
3.6.1 Proposed Encryption Evaluation Method 56
3.6.2 Scaling and Scoring for SPN Configuration Result 62
3.7 New Hash Function Algorithm 65
3.8 Proposed Hash Function Evaluation Method 67
3.9 Summary 70

CHAPTER 4 KEYSPACE EVALUATION OF CHAOS-BASED CRYPTOGRAPHIC ALGORITHMS 71

4.1 Introduction 71

4.2 Attack Model and Other Assumptions 71

4.3 Keyspace Analysis of Chaos-based Encryption 73

4.3.1 Low Energy Interleaved Chaotic Secure Image Coding Scheme for Visual Sensor Networks Using Pascal's Triangle Transform 74

4.3.2 Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding 76

4.3.3 New Image Encryption Algorithm with Nonlinear-Diffusion Based on Multiple Coupled Map Lattices 80

4.3.4 A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing 82

4.3.5 RGB Image Encryption Through Cellular Automata, S-Box and the Lorenz System 84

4.3.6 A Robust and Fast Image Encryption Scheme Based on a Mixing Technique 86

4.3.7 A Novel Chaotic Image Encryption Algorithm Based on Extended Zigzag Confusion and RNA Operation 89

4.3.8 An Effective Image Encryption Algorithm Based on Compressive Sensing and 2D-SLIM 91

4.4 Secret Key Recommendations 93

4.5 Key Schedule 96

4.6 Summary 98

CHAPTER 5 DESIGN OF THE CHAOS-BASED ENCRYPTION ALGORITHM 100

5.1 Introduction 100

5.2 Selection of Chaotic Map 101

5.3 SPN Comparison of Configuration Operations 102

5.4 SPN Cipher Design 102

5.5 Experimental Evaluation of SPN 104

5.5.1 Analysis of Findings 138
5.5.2 Top Five (5) Best Configurations Based on the Experiment 140
5.6 Summary 141
CHAPTER 6 PROPOSED CHAOTIC FEISTEL BLOCK CIPHER (CFBC) 142
6.1 Introduction 142
6.2 CFBC Design 143
6.2.1 Key Schedule 143
6.2.2 Nonlinearity Function 144
6.2.3 Diffusion Function 145
6.2.4 Ciphertext Randomness Test 145
6.2.5 Security against Differential Cryptanalysis 148
6.3 An Image Encryption Scheme Based on CFBC 149
6.3.1 Round Key Generation Phase 150
6.3.2 Image Encryption Phase 151
6.3.3 Histogram Analysis 153
6.3.4 Correlation Coefficient Analysis 155
6.3.5 Information Entropy 157
6.3.6 NPCR and UACI Analysis 158
6.3.7 Comparison with Existing Works 159
6.4 A Chaos-based Hash Function Based on CFBC 160
6.4.1 Compression Function of Proposed Hash Function 161
6.4.2 Experimental Evaluation 162
6.4.3 Sensitivity Test 162
6.4.4 Diffusion and Confusion Test 164
6.5 Summary 166
CHAPTER 7 CONCLUSION AND FUTURE WORK 167
7.1 Summary and Contributions 167

7.2 Future Work 170

REFERENCES..... 172

APPENDICES

LIST OF PUBLICATIONS

LIST OF TABLES

Page

Table 1.1	Research Methodology	11
Table 2.1	Relationship Between Chaotic System and Cryptographic Algorithm (Gonzalo Alvarez & Li, 2006)	22
Table 2.2	Comparison Between 1D and HD Chaotic Map	29
Table 2.3	Recent Chaos-Based Encryption Algorithms and Their Problems	45
Table 2.4	Recent Chaos-Based Hash Functions and Their Problems	45
Table 3.1	Block Shuffle	54
Table 4.1	Summary of Keyspace Reductions (Measured in Bits)	94
Table 4.2	NIST SP 800-22 Results	98
Table 4.3	ENT Test Results	98
Table 5.1	Top 5 Result Using Logistic Map Before Resetting Initial Condition and Control Parameter	106
Table 5.2	Average Score of the Three (3) Images in Table 5.1	108
Table 5.3	Top Five (5) Result Using Logistic Map After Resetting Initial Condition and Control Parameter	110
Table 5.4	Average Score of the Three (3) Images in Table 5.3	112
Table 5.5	Top Five (5) Result Using Tent Map Before Resetting Initial Condition and Control Parameter	114
Table 5.6	Average Score of the Three (3) Images in Table 5.5	116
Table 5.7	Top Five (5) Result Using Tent Map After Resetting Initial Condition and Control Parameter	118
Table 5.8	Average Score of the Three (3) Images in Table 5.7	120
Table 5.9	Top Five (5) Result Using 2D Piecewise Linear Map Before Resetting Initial Condition and Control Parameter	122
Table 5.10	Average Score of the Three (3) Images in Table 5.9	124
Table 5.11	Top Five (5) Result Using 2D Piecewise Linear Map After Resetting Initial Condition and Control Parameter	126

Table 5.12 Average Score of the Three (3) Images in Table 5.11 128

Table 5.13 Top Five (5) Result Using 2D Henon Map Before Resetting Initial Condition and Control Parameter 130

Table 5.14 Average Score of the Three (3) Images in Table 5.13 132

Table 5.15 Top Five (5) Result Using 2D Henon Map After Resetting Initial Condition and Control Parameter 134

Table 5.16 Average Score of the Three (3) Images in Table 5.15 136

Table 5.17 Best Optimum Configuration, (S: Substitution and P: Permutation) 140

Table 6.1 CFBC NIST SP 800-22 Result 147

Table 6.2 ENT Test 148

Table 6.3 Histogram Analysis of The Proposed Scheme 154

Table 6.4 Correlation Coefficient of Proposed Scheme 156

Table 6.5 Entropy Analysis of Proposed Scheme 158

Table 6.6 NPCR and UACI Result 159

Table 6.7 Comparison of Proposed Cipher Against Other Existing Image Ciphers 160

Table 6.8 Diffusion and Confusion Analysis for The Proposed Hash Function 165

Table 7.1 Summary of Findings and Results 170

LIST OF FIGURES

Page

Figure 1.1	Research Overview	12
Figure 2.1	SPN Structure	17
Figure 2.2	Feistel Structure	18
Figure 2.3	SPECK Structure	19
Figure 2.4	Sponge Construction	20
Figure 2.5	Davis-Meyer Construction	20
Figure 2.6	Logistic Map Iterating Function	24
Figure 2.7	(a) Bifurcation Diagram of Logistic Map and (b) Lyapunov Exponent of Logistic Map	27
Figure 2.8	(a) Bifurcation Diagram of Tent Map and (b) Tent Map Lyapunov Exponent	28
Figure 2.9	Bifurcation Diagram for Logistic Map	33
Figure 2.10	Divergence of Distance for Nearby Two Orbits (Zhou & Wang, 2021)	34
Figure 2.11	Histogram of Logistic Map for Different Values of Control Parameter (a) = 4, (b) = 3.89472 (Arroyo et al., 2008)	35
Figure 3.1	The General Structure of the Proposed Research	48
Figure 3.2	The Proposed Key Schedule	51
Figure 3.3	Chaotic Feistel Block Diagram	53
Figure 3.4	C-Function	53
Figure 3.5	Structure of the Proposed Image Encryption Scheme	55
Figure 3.6	Davies-Meyer Construction	66
Figure 4.1	Flowchart of the Encryption Process for Suseela et al., (2021)	75
Figure 4.2	Flowchart of the Encryption Process for Belazi et al., (2019)	78
Figure 4.3	Flowchart of the Encryption Process for Wang et al., (2019)	81

Figure 4.4 Flowchart of the Encryption Process for (Lidong et al., 2020) 83

Figure 4.5 Flowchart of the Encryption Process for (Alexan et al., 2022) 85

Figure 4.6 Flowchart of the Encryption Process for (Heucheun Yepdia et al., 2021) 88

Figure 4.7 Flowchart of the Encryption Process for Wang and Guan, (2020)..... 90

Figure 4.8 Flowchart of the Encryption Process for Xu et al., (2020)..... 92

Figure 4.9 Proposed Key Schedule 97

Figure 5.1 Histogram Results of Test Images and Their Cipher Histograms Using First Optimal Configuration Operation (SPS) Based on Logistic Chaotic Map. 105

Figure 6.1 Proposed CFBC 143

Figure 6.2 Framework of the Proposed Image Encryption Scheme 150

Figure 6.3 Secret Key Generation..... 151

Figure 6.4 Histogram Results of Test Images and Their Cipher Histograms Using the Proposed Scheme..... 155

Figure 6.5 Correlation Coefficient Analysis for Images (Cameraman, Lena, Peppers and 5.1.10), Plain and Cipher Images in Horizontal, Vertical and Diagonal Directions 157

Figure 6.6 Proposed Hash Function Based on CFBC..... 161

Figure 6.7 128 Bits Hash Values of Different Five Cases 163

Figure 6.8 Distribution of Changed Bit Number and its Histogram..... 165

LIST OF ABBREVIATIONS

1D	One-Dimension
2D	Two-Dimension
AES	Advanced Encryption Standard
ARX	Addition Rotation Exclusive-OR
CBC	Cipher Block Chaining
CCM	Combination of Chaotic Maps
CD	Correlation Dimension
CFBC	Chaotic Feistel Block Cipher
CFS	Chaotic Feistel Structure
CPU	Central Processing Unit
CTR	Counter
DC	Design Complexity
DDT	Differential Distribution Table
DES	Data Encryption Standard
DWT	Discrete Wavelet Transformation
GB	Gigabyte
GB	Gigabyte
GFS	Generalized Feistel Structure
GHZ	Gigahertz
HCC	Higher Computational Cost
HD	Higher Dimension
IKJ	Inaccurate Keyspace Justification
IPsec	Internet Protocol Security
LE	Lyapunov Exponent

LFSR	Linear Feedback Shift Register
LLE	Large Lyapunov Exponent
LSB	Least Significant Bit
MD5	Message-Digest Five
MSB	Most Significant Bit
NIST	National Institute of Standards and Technology
NPCR	Number of Pixel Change Rate
NSA	National Security Agency
PDF	Probability Distribution Function
PRNG	Pseudo Random Number Generator
PTT	Pascal Triangle Transformation
PWLCM	Piecewise Linear Chaotic Map
SA	Security Association
SE	Shannon Entropy
SPN	Substitution Permutation Network
TLS	Transport Layer Security
TRNG	True Random Number Generator
UACI	Unified Average Change Intensity

LIST OF APPENDICES

APPENDIX A PRELIMINARY WORK ON COMPARISON OF DESIGN PARADIGMS AND CHAOTIC MAPS

PARADIGMA REKA BENTUK KEBOLEHANALISIS BERASASKAN CAMUK UNTUK APLIKASI KRIPTOGRAFI

ABSTRAK

Kriptografi berasaskan camuk telah mendapat perhatian yang ketara, dengan banyak reka bentuk memfokuskan pada mengaburi keselamatan melalui reka bentuk kompleks yang menyukarkannya untuk dianalisis, struktur reka bentuk yang tidak betul (reka bentuk ad-hoc) dengan justifikasi ruang kekunci yang tidak tepat. Ini menjejaskan piawaian prinsip reka bentuk yang direka dengan baik, mudah dan selamat dalam protokol reka bentuk kriptografi dan tidak memudahkan usaha kriptanalitik masa hadapan. Lebih-lebih lagi, sehingga kini, belum ada sebarang sistem kriptografi berasaskan camuk yang dilaksanakan untuk menjamin komunikasi dunia sebenar. Kajian ini mencadangkan paradigma mudah dan boleh dianalisis berdasarkan prinsip kriptografi yang mantap (SPN dan Feistel) untuk menangani isu ini. Pertama, semakan mendalam dijalankan ke atas terkini terkini dalam bidang algoritma kriptografi berasaskan camuk untuk mengenal pasti cabaran pelbagai kaedah reka bentuk dan penilaian yang telah dibangunkan selama ini. Analisis menyeluruh terhadap masalah yang diabaikan dalam sistem kripto berasaskan camuk dijalankan, menonjolkan ruang kekuncinya yang luar biasa besar. Pelbagai contoh menunjukkan contoh sifir berasaskan camuk yang melebihkan ruang kekunci dan mendedahkan cabaran praktikal dan teori dalam pendekatan penjanaan utama. Kajian itu mengetengahkan cadangan dan penyelesaian alternatif untuk menggunakan kunci rahsia dalam kriptografi berasaskan camuk. Kemudian, jadual kunci berasaskan camuk ringkas yang memastikan penglibatan setiap bit kunci rahsia dalam penjanaan kunci bulat dicadangkan. Jadual utama yang dicadangkan berjaya melepasi kedua-dua suite

ujian statistik NIST dan ENT, menunjukkan bahawa reka bentuk yang sangat kompleks tidak diperlukan untuk mencapai sifat keselamatan yang diingini. Penyelidikan selanjutnya menyiasat kesan operasi asas (penggantian dan pilih atur) pada keputusan statistik untuk proses penyulitan. Eksperimen dijalankan untuk membandingkan dan memilih konfigurasi operasi yang optimum berdasarkan tanggapan kekeliruan dan resapan. Kajian ini juga menyiasat lebih lanjut pengaruh dan kesan penggunaan pelbagai camuk (peta 1 dimensi dan 2 dimensi) dan menunjukkan bahawa menukar peta mempunyai kesan minimum pada keputusan statistik selagi peta beroperasi dalam kawasan camuknya. Kemudian, konfigurasi terbaik digunakan untuk mereka bentuk algoritma penyulitan yang mudah tetapi mantap untuk menyiasat keselamatan dan kepraktisan kaedah yang dicadangkan, dengan mengambil kira kebolehanalisisan sebagai matlamat kajian. Akhirnya, sifir Feistel (CFBC) berasaskan camuk baru dicadangkan. Sifir yang dicadangkan mencapai keputusan statistik yang baik, menunjukkan potensinya untuk aplikasi kriptografi yang selamat. Sebagai bukti konsep, CFBC digunakan untuk mereka bentuk sifir imej dan fungsi cincang, kedua-duanya mempamerkan sifat statistik yang mantap dan keselamatan yang dipertingkatkan berbanding dengan algoritma camuk sebelumnya yang direka bentuk secara berbelit-belit. Oleh itu, memajukan potensi kebolehgunaan algoritma kriptografi berasaskan camuk dalam senario dunia sebenar.

ANALYSABLE CHAOS-BASED DESIGN PARADIGMS FOR CRYPTOGRAPHIC APPLICATIONS

ABSTRACT

Chaos-based cryptography has garnered significant attention, with many designs focusing on obscuring security through complex designs that make them difficult to analyze, improper design structures (ad-hoc designs) with inaccurate keyspace justification. These compromise the standards of well designed, simple, and secure design principles in cryptographical design protocol and do not facilitate future cryptanalytic efforts. Moreover, to date, there have not been any chaos-based cryptosystems being implemented to secure real-world communications. This study proposes simple and analyzable paradigms based on well-established cryptographic principles (SPN and Feistel) to address these issues. First, an in-depth review is conducted on the current state-of-the-art in the field of chaos-based cryptographic algorithms to identify the challenges of various design and evaluation methods that have been developed over the years. A comprehensive analysis into a largely overlooked problem in chaos-based cryptosystems is conducted, highlighting their unusually large keyspaces. Multiple examples demonstrate instances of chaos-based ciphers overestimating keyspaces and reveal practical and theoretical challenges in key generation approaches. The study highlights recommendations and alternative solutions for utilizing secret keys in chaos-based cryptography. Then, a simple chaos-based key schedule that ensures the involvement of every bit of the secret key in the generation of round keys is proposed. The proposed key schedule successfully passed both the NIST and ENT statistical test suites, indicating that highly complex designs are unnecessary to achieve desirable security properties. The research further

investigates the impact of basic operations (substitution and permutation) on statistical results for encryption processes. Experiments are conducted to compare and select optimal configurations of operations based on the notion of confusion and diffusion. The study also further investigates the influence and impact of using different chaotic (1-dimensional and 2-dimensional maps) and shows that changing the map has minimal impact on statistical results as long as the map is operating within its chaotic region. Then, the best configuration is used to design simple yet robust encryption algorithm to investigate the security and practicality of the proposed method, keeping in mind analyzability as the goal of the study. Finally, a novel chaos-based Feistel cipher (CFBC) is proposed. The proposed cipher achieved a good statistical result, indicating its potential for secure cryptographic applications. As a proof of concept, CFBC is used to design an image cipher and a hash function, both exhibiting robust statistical properties and enhanced security compared to previous chaotic algorithms designed in convoluted manner. Thus, advancing the potential applicability of chaos-based cryptographic algorithms in real-world scenario.

CHAPTER 1

INTRODUCTION

1.1 Background

With the rapid development of digital technology today, users' data of any kind are available on the internet which may contain confidential and sensitive information regarding business, medical records, military affairs, and other crucial information. In this regard, the protection of such sensitive information is very much essential for any organization or individual so that it cannot be compromised by unauthorized access. To protect this media against cyberattacks for safe data transmission, efficient cryptographic algorithms are required to maintain security over unrestricted public channels (data-in-transit) and data-at-rest.

Cryptography is the study of mathematical approaches connected to aspects of information security such as confidentiality, data integrity, and entity authentication. Cryptography provides the means to ensure that the data being transmitted must be kept secret, correct, and to the right receiver, as well as ensuring that the sender and receiver are whom they claim to be. The opposite of cryptography is cryptanalysis. Cryptanalysis is the study of decrypting cipher data without having access to the key.

The plaintext is the message before it is encrypted in any way, while the ciphertext is the encrypted message. Encryption involves hiding the content of a message by obscuring it. Decryption, on the other hand, is a procedure of converting ciphertext back to plaintext. The cryptographic algorithm and the key are two components required for encryption and decryption. The key is a piece of information that governs how the cryptographic algorithm operates and produces a unique result

for a specific user, and the cryptographic algorithm is the mathematical function used to encrypt and decode the message. Encryption is often the first thing that springs to mind when someone mentions cryptography. However, cryptography covers a wide range of areas including message authentication and integrity. Ciphers are mathematical methods that convert the original data (plaintext) into a separate set of data (known as ciphertext) that has no resemblance to the plaintext. This transformational process, known as encryption, takes place at the beginning of a communication channel and makes use of the key mentioned above. Cryptographic algorithms are widely used in the field of information security and networking environments. With the increasing demand for data security, many scholars have proposed many encryption techniques and algorithms (Bouteghrine et al., 2021; Liu et al., 2020; Luo et al., 2019; Pan et al., 2018).

Chaos theory is a branch of mathematics that deals with nonlinear systems exhibiting the butterfly effect, in which a minor change in a system's initial condition can result in huge changes in its outputs. Population, climate, and road traffic are all examples of chaotic systems that could be observed. Chaos has been used to design image encryption, hash functions, and other chaos-based applications (Teh et al., 2020). Chaos has shared properties (nonlinearity, sensitivity to initial conditions, ergodicity, and unpredictability) with cryptography that motivate their adoption in the design of algorithms like image ciphers and hash functions.

Chaos-based cryptographic algorithms rely on chaotic maps as a source of randomness. These chaotic maps are an alternative source of randomness to commonly used methods like the Linear Feedback Shift Register (LFSR) which operates based on an initial value called a seed and has a finite number of possible states to create a pseudorandom number stream. The random number generator is needed to have a

sufficiently fast generation speed to aid in achieving fast encryption. At the same time, the randomness of the key remains essential to the security of an encryption system. Some researchers have adopted chaotic random number generators in cryptosystems, attracted by the uncertainty, non-repeatability, and unpredictability inherent in chaotic systems (Man et al., 2021).

1.2 Problem Statement

Although many chaos-based cryptosystems have been designed in the past decade, (Luo et al., 2019; Yu et al., 2019; Tutueva et al., 2020; Liu et al., 2020; Bouteghrine et al., 2021) many of these algorithms suffer from lack of design paradigms with proper underlying security principles (Ljupco Kocarev, 2001; Murillo-Escobar et al., 2019). There is also lack of well-established design paradigms, unlike conventional cryptography which has the substitution-permutation network (SPN), Feistel structure, addition-rotation-XOR (ARX) and so on. The design of many chaos-based algorithms run contrary to the commonly accepted design principle of cryptographic algorithms, which emphasizes simple, analyzable designs with well-defined design rationale (Murillo-Escobar et al., 2019; Rani, 2018; Teh et al., 2020). Therefore, most of these algorithms are not utilized in practical applications and lack real world impact. Particularly, they often lack the rigorous third-party cryptanalysis commonly conducted on conventional ciphers (Bardeh & Rijmen, 2022; Boura et al., 2023; Dey et al., 2023; Nyberg, 2021) demonstrating the necessity for thorough cryptanalysis to evaluate their claimed security margins and suitability for practical use.

This thesis starts by addressing one of the lesser-studied problems in chaos-based cryptography, which is the security of their key schedule. One of the problems

of chaos-based primitives in cryptography lies in their tendency to emphasize unusually large keyspaces as a measure of security. Researchers often claim that larger keyspaces provide greater security against attacks (Ali & Ali, 2020; Ge et al., 2021; Hanif et al., 2020; H. Li et al., 2019; Luo et al., 2019; Yasser et al., 2022). Although a larger keyspace is commonly considered desirable, it is important to note that the security of an algorithm cannot be solely determined by the length of its key. The notion of computational or conditional security plays a crucial role in determining the security of a cipher. A cipher is deemed secure if the most efficient cryptanalytic attack needs computational complexity that is equal to or greater than an exhaustive key search. Therefore, the focus should not solely be on key length, but rather on the algorithm's resistance against known attacks and its ability to withstand exhaustive key search efforts.

Furthermore, the evaluation of keyspace in chaos-based primitives is not always accurate, leading to potential misconceptions regarding the actual level of security. Moreover, some studies have highlighted that the effective use of keys in the encryption process is crucial for achieving strong security, rather than solely relying on the size of the keyspace. The overemphasis on large keyspaces without proper utilization of the keys can lead to a false sense of security (G. Alvarez & Li, 2009; Teh, Alawida, & Sii, 2020). As such, the need for a more comprehensive and accurate evaluation of keyspace in chaos-based cryptographic systems is fundamental.

Most chaos-based algorithms rely on security through obscurity which makes them needlessly complex and difficult to analyze. Obscurity is the reliance on design secrecy as the main method of providing security to a system (Arroyo et al., 2009). This complexity not only hinders analysis but also undermines confidence in the cryptosystems' real-world viability. Many researchers today propose new, complex

chaotic maps with the purpose of improving security (Arroyo et al., 2009; Hosseinzadeh et al., 2019; Wang et al., 2019). This method makes it difficult for researchers who are aiming to use cryptanalytic methods to verify the security claims. This can further hide the security weaknesses from the designers themselves, making it difficult to verify any security claims. This will result to a lack of confidence in these cryptosystems for real-life applications. Many chaos-based cryptosystems still do not address major implementation problems which include complex design, computational complexity analysis, lack of efficiency analysis among others (Teh et al., 2020). Majority of chaos-based cryptographic algorithms are proposed based on multiple chaotic maps, hyperchaotic maps, and other complicated designs (Li et al., 2018; Pak & Huang, 2017).

However, despite passing all the statistical tests they have been successfully cryptanalyzed (Chen et al., 2018; Hu et al., 2017; Huang et al., 2020; Li et al., 2019; Liu et al., 2019; Norouzi & Mirzakuchaki, 2017; Preishuber et al., 2018; Wang et al., 2018; Wen et al., 2019; Zhang et al., 2017; Zhang, 2020; Zhu & Sun, 2018). Thus, a shift towards less complex primitives in chaos-based cryptography is fundamental to enable rigorous security analysis and build trust for real-world applications.

In this research, the following research questions will be addressed:

- How can a chaos-based cryptosystem be designed to facilitate cryptanalysis?
- How can a chaos-based key schedule be designed to ensure equal participation of all key bits in enhancing security?

- What well-studied cryptographic paradigms can be used to design chaos-based cryptosystems?

- How can a chaos-based cryptosystem be designed to minimize design complexity while maintaining good security properties?

1.3 Research Motivation

Chaos theory has the potential to be used to develop strong cryptographic primitives due to its various desirable properties. However, with how the general research direction is going, this goal is still not achieved in the near future. Therefore, there is a need to shift the research focus. The ease of analysis is important in ensuring that cryptanalysis efforts can be conducted to verify the security claims and to accurately measure their security margins. Each part of the design should be made known, especially in the documentation (Teh et al., 2020). Existing chaotic-based schemes lack real-world impact. Hence, a chaos-based algorithm designed using simple, analysable, and well-studied paradigms which adapt notions of confusion and diffusion serves as a pace setter for future chaos-based research.

Statistical methods in general have been used to determine if a cipher is resistant to attacks, these methods are based only on the cipher output and disregard the cipher's structure. A secure design should be also statistically sound, but being statistically sound does not imply a secure design (Teh et al., 2020). When new cryptosystems such as new block ciphers, stream ciphers, hash functions, or authenticated ciphers, are introduced, their designers originally subject them to early cryptanalysis. To cryptanalyze a design, one must first understand the behaviour and properties of the cryptosystem. This creates confidence in a cryptosystem and

facilitates future cryptanalysis efforts by other researchers. Thus, if the objectives of this work are achieved, chaos-based cryptographic algorithms are one step closer to seeing real-world applications.

1.4 Research Objectives

The main goal of this research is to contribute towards the advancement of chaos-based cryptographic algorithms from the perspectives of both design and analysis of their security. In terms of security analysis, the proposed work investigates security claims from the perspective of key schedule design. In terms of design, the thesis first introduces an alternative key schedule design that addresses the problems found during cryptanalysis, then move on to propose new designs of chaos-based cryptographic algorithms, both of which focus on reducing design complexity without compromising security. This is achieved by adapting general purpose designs. This contrasts with existing chaos-based algorithms today that have complex designs or rely on complex chaotic maps to improve security. This approach makes using cryptanalytic methods to verify security claims difficult. The main objectives of this research can be broken down into three research objectives:

i. To cryptanalyse the key schedules of existing chaos-based encryption algorithms to provide more accurate security estimates.

ii. To propose a new chaos-based key schedule that is both secure and ensures that each key bit plays an equal role in providing security.

iii. To propose cryptographic design paradigms which can be used for chaos-based cryptographic algorithms.

1.5 Research Contributions

The achievement of the research objectives results in numerous contributions to the field of cryptography. Firstly, showcasing that keyspaces of chaos-based ciphers have been over-estimated, bringing attention to the practical and theoretical challenges associated with their key generation approaches. Then highlighting alternative solutions to how secret keys can be used in the context of chaos-based cryptography. Secondly, proposing a key schedule for chaos-based ciphers that ensures the involvement of every bit of the secret key in the generation of round keys. Thirdly, developing new cryptographic design structures for chaos-based cryptography based on well-established design paradigms with strong underlying principles and proper security justification. The approaches are based on the well-accepted design principle of cryptographic algorithms, which emphasizes simple, analyzable designs with well-defined design rationale. These structures aim to provide a new direction for future researchers in chaos-based cryptography. By adopting extensively analyzed constructs like the Feistel network or Davies-Meyer construction, chaos-based cryptosystems could potentially see real-world applications.

The fourth contribution is the design and analysis of new chaos-based cryptosystems. The cryptosystems are designed to be simple, analyzable, and secure while utilizing chaos as an underlying source of randomness. These cryptosystems include an encryption algorithm and hash function. The contributions of this work can be summarized as follows:

i. Accurate keyspace evaluation of existing chaos-based algorithms, providing more accurate security estimates.

ii. New key schedule that is secure and ensures that each key bit plays an equal role in providing security.

iii. New cryptographic design paradigms that can be used for encryption and data integrity algorithms.

iv. A new encryption algorithm that is both secure and analyzable based on the proposed design paradigms.

v. A new hash function algorithm that is both secure and analyzable based on the proposed design paradigms.

1.6 Scope of the Research

This thesis studies chaos-based cryptography, with a focus on encryption and integrity algorithms. A deep look into some recent existing chaos-based algorithms from the perspective of the secret key is conducted. The analysis provides actual security margins of these ciphers with a more accurate keyspace estimate. Some alternative solutions to how secret keys can be used in the context of chaos-based cryptography are highlighted and a simple key schedule is proposed. The goal is to bring to light yet another problem of chaos-based cryptography that needs to be addressed in future research to advance the field in the right direction.

The block cipher proposed in this work relies on 1-dimensional chaotic maps such as logistic and tent maps. These maps are simple and commonly used maps in cryptosystems design and help maintain the simplicity of the resulting cryptosystems.

Furthermore, the proposed block cipher and hash function are investigated for security and practicality. The block cipher's design simplicity allows for evaluation

against cryptanalytic attacks such as differential cryptanalysis. The cipher is designed to accommodate all data types. However, comparisons and experiments are performed using images because nearly all recently proposed chaos-based ciphers are image ciphers.

1.7 Research Methodology

This section presents an overview of the research methodology. First, an in-depth review is performed on the current state of the art in the field of chaos-based cryptographic algorithms to identify the challenges of various design methods and approaches. Existing work on symmetric-key encryption and hash functions are examined to determine if recently proposed algorithms still suffer from the previously mentioned drawbacks in terms of inaccurate keyspace, design complexity or improper design paradigms, as well as to identify the various strategies that can be used to design simple yet secure algorithms that are justified by cryptographic principles. Then, an in-depth review of cryptanalysis methods is performed to identify loopholes and weaknesses of previous chaos-based cryptographic algorithms. Finally, the research moves on to investigate various statistical-based cryptanalysis approaches that have been developed over the years to ensure the designed cryptosystems are resistant against the state-of-the-art cryptanalysis.

Next, the research moves to provide several examples of recent chaos-based cryptographic algorithms with keyspace issues, evaluate their effective keyspaces security claims and highlights an approach in addressing these issues. A simple key schedule that ensures the involvement of each key bit in encryption process is proposed and evaluated using the standard statistical test suites.

Then, the research proceeds to propose and test chaos-based design paradigms based on conventional ones such as SPN keeping in mind analysability as the goal of the study. Testing is performed using statistical tests that are commonly used in chaos-based cryptography. The research investigates the impact of basic operations (substitution and permutation) on statistical results of the encryption process. Experiments are carried out to compare and select optimal configurations of operations based on the notion of confusion and diffusion. The study also further investigates the influence and impact of using different maps (1-dimensional and 2-dimensional maps) and shows that changing the map has minimal impact on statistical results as long as the map is operating within its chaotic region. Standard images are used for the experiment testing for fair comparison with other chaos-based ciphers. The best configuration is presented which can be used to design simple yet robust encryption algorithms. The overview of the research methodology is shown in Table 1.1 while Figure 1.1 illustrates the roadmap of the research.

Table 1.1 Research Methodology

Steps	Research Objective
1. Literature study i. 1-D and 2-D chaotic maps ii. Design of encryption and hash function algorithms.	All related objectives
2. Keyspace analysis of existing chaos-based encryption algorithms.	To cryptanalyse the key schedules of existing chaos-based encryption algorithms to provide more accurate security estimates.
3. Design of key schedule with effective utilization of key bit based on chaotic system.	To propose a new chaos-based key schedule that is both secure and ensures that each key bit plays an equal role in providing security.
4. Evaluation of design structures i. SPN ii. Feistel iii. Davies Meyer Construction	To propose cryptographic design paradigms which can be used for chaos-based cryptographic algorithms.

Table 1.1 (Continued)

Steps	Research Objective
5. Design of chaos-based block cipher based on design structures in (4). 6. Evaluation of the chaos-based block cipher	To propose an analyzable chaos-based encryption algorithm based on the newly proposed design paradigms.
7. Design of a chaos-based hash function based on (5). 8. Evaluation of the chaos-based hash function	To propose an analyzable chaos-based cryptographic hash function based on the newly proposed design paradigm.

Then, chaos-based Feistel cipher (CFBC) is proposed, representing a new variant of the generalized Feistel network. Finally, an encryption and a hash function algorithm are designed based on the new proposed block cipher. The hash function is constructed using Davies-Meyer construction, as it offers a straightforward approach to construct a secure hash function from a block cipher. A detailed look at the research methodology is provided in Chapter 3.

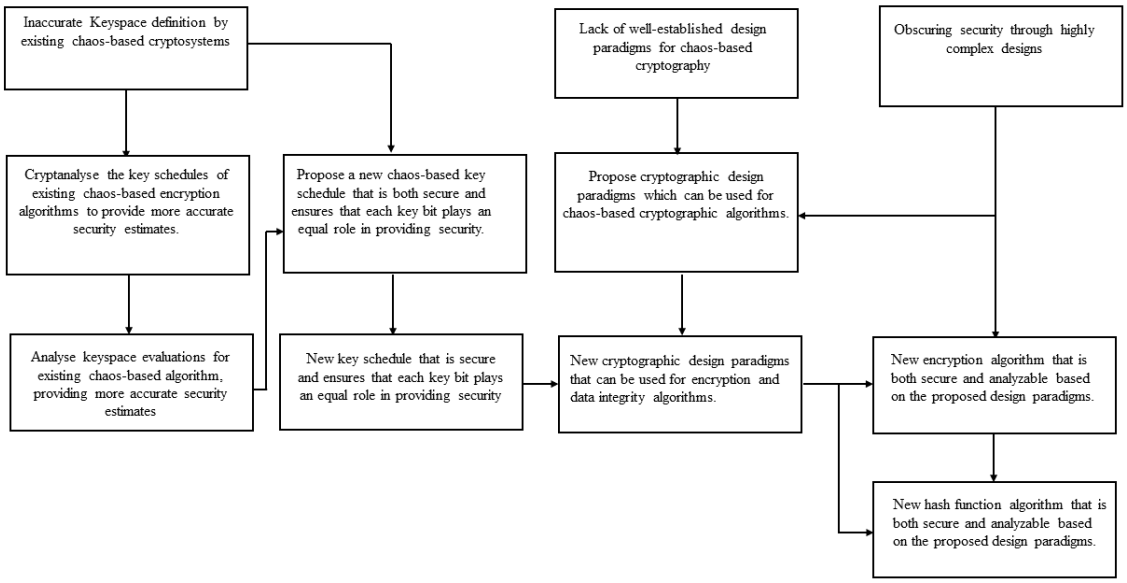

Figure 1.1 Research Overview

1.8 Organization of Thesis

The problem statement, research questions, motivation, and objectives were discussed in this chapter. These are essential to understand the existing problems that motivate and inspire this work. The chapter also provides an overview of the research methods that are employed in order to achieve the aims of the research work. Chapter 2 briefly reviews the previous related literature in the field of chaos-based cryptography, highlighting the problem of existing convoluted designs. Reviews of existing cryptosystems algorithms (image encryption and hash function) are discussed in this chapter. A detailed description of the research methodology is then provided in Chapter 3.

An analysis of keyspace of various existing chaos-based ciphers which reveals that their security claims have been overestimated is detailed in Chapter 4. This analysis provides accurate keyspace estimates for these ciphers and highlights alternative solutions for how secret keys can be used in the context of chaos-based cryptography, proposing a simple key schedule as proof of concept. Following that, Chapter 5 delves deeply into the comparison configurations of the substitution-permutation network (SPN) design paradigm, using different chaotic maps.

Chapter 6 discusses the proposed chaos-based Feistel cipher (CFBC). The block cipher is used to design an image cipher as well as a hash function. Due to its design simplicity, the block cipher can be evaluated against cryptanalytic attacks such as differential cryptanalysis. Chapter 7 concludes the thesis and outline some ideas for future research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Today, there is rapid acceleration in sharing of data/information in critical sectors like health care, military, social media, e-commerce, e-governance, and so on. Securing private multimedia information by providing confidentiality, integrity, and ownership of identity has become a critical and vital issue when sensitive information is transferred across open internet channels. Cryptography is a term used to describe secure information and communication techniques that use mathematical concepts and a set of rule-based calculations known as algorithms to transform messages in difficult ways to decipher. The major goals of cryptography can be categorized as confidentiality, data integrity, authentication, and non-repudiation (Khalifa et al., 2004; Zhang et al., 2011). The general concept of cryptography can be described as Follows: Let P and C stand for the plaintext and ciphertext, respectively. An encryption algorithm can be described as $C = E_{Ke}(P)$. where *Ke* is the encryption key and *E* is the encryption function. Hence, $P = D_{Kd}(C)$, where *Kd* is decryption key and *D* is the decryption function.

Symmetric cryptography addresses the problem of secrecy protection by using a shared secret key (*Ke = Kd)* to transform a message in such a way that it cannot be easily recovered without the key. This process is called symmetric-key or symmetric encryption. Algorithms that perform symmetric encryption are known as ciphers. Based on how messages are encrypted, these ciphers are typically categorized into one of two classes: block ciphers and stream ciphers. Symmetric-key cryptosystems are fast and efficient, and they are best-suited for encrypting large amounts of data at a

high speed (Gonzalo Alvarez & Li, 2006). This thesis focuses on symmetric-key cryptosystems.

A cryptographic hash function maps a message string of any length to a fixed length string known as a hash value. Hash functions are widely used to search duplicates in data sets, for secure storage of passwords, and implementing electronic digital signatures (Tutueva et al., 2020). There are two types of hash functions: keyed and unkeyed. When given the same input, an unkeyed hash function produces the same output, whereas a keyed hash function combines the key information into the hash value, resulting in different hash values when different keys are used. MD5 and SHA-1 are two examples of conventional hash functions, with digest size of 128 and 160 bits, respectively (Kessler, 2019). Over the past decade, many chaos-based hash functions have been proposed (Abdoun et al., 2020; Assad et al., 2020; Alawida et al., 2021; Liu et al., 2021; Liu et al., 2020; Naor & Yung, 1989; Teh et al., 2020; Xiao, 2005).

Security is a prime goal in cryptographic design. To ensure real-world security and efficiency, algorithms should be designed to be analyzable, while still providing the claimed level of security. Simplicity is an effective catalyst that enables compact implementations and enhances communication.

2.2 Design Paradigms

The convoluted manner in which most chaos-based cryptosystems are designed is one of the most common problems in the field. The majority of designs concentrate on highly complicated structures with the aim of causing problems for adversaries

attempting to analyze them. Instead, a chaos-based cryptosystem should be designed using well-understood cryptographic principles (MySEAL, 2018; Teh et al., 2020).

In the 1940s, Claude Shannon highlighted the importance of confusion and diffusion for a cryptosystem (Shannon, 1948, 1949). Confusion is the property of obscuring the relationship between plaintext and ciphertext elements, whereas diffusion is the spreading of plaintext elements' influence over ciphertext elements. Shannon suggested a mixing transformation involving several rounds, with each round consisting of a substitution operation followed by an invertible linear transformation. This has led to the introduction of several well-known design structures that all adopt these basic principles, including SPN, Feistel and ARX structures.

2.2.1 Substitution-Permutation Network (SPN)

SPN can be used to achieve the practical realization of Shannon's mixing transformation (Dawood, 2020; Feistel, 1973; Hue et al., 2012). SPN is a type of block cipher that is made up of rounds of a repetitive series of mathematical operations. SPN is a significant class of private key cryptosystem. It takes a block of plaintext and a key as inputs and applies several alternating rounds of substitution and permutation to generate each block of ciphertext output (Keliher et al., 2000). The key bits are mixed with those of the plaintext during the non-linear substitution stage, which results in Shannon's confusion. After that, redundancies are eliminated by the linear permutation stage, resulting in diffusion. (Noura et al., 2018). AES (Daemen & Rijmen, 2002), 3-Way (Daemen et al., 1994), and PRESENT (Bogdanov et al., 2007) are examples of ciphers based on SPN.

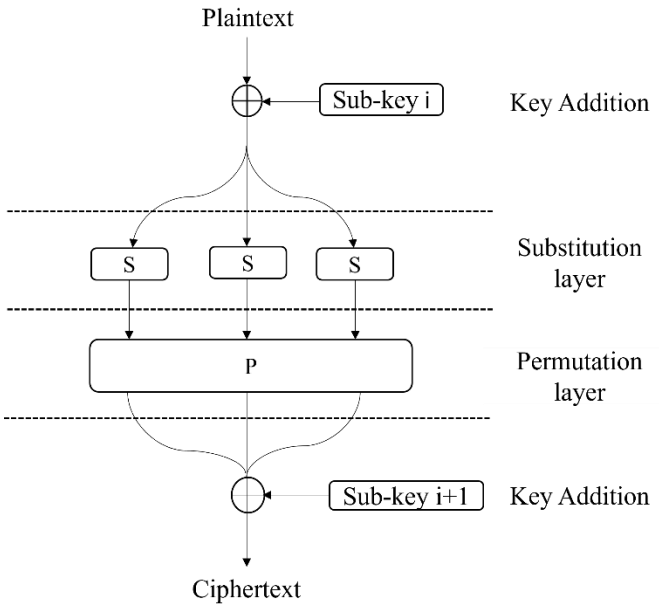

Figure 2.1 SPN Structure

2.2.2 Feistel Network

The Feistel network uses a round function, which takes two inputs (a data block and a subkey), and returns an output of the same size as the data block (Stinson & Paterson, 2019). In each round, the round function is applied to half of the data to be encrypted, and the output is XORed with the other half of the data. This procedure is repeated several times, with the encrypted data as the final output. (Schneier, 1996). The Feistel cipher combines elements of substitution, permutation, transposition, and key expansion, resulting in significant confusion and diffusion. Another advantage of Feistel designs is that the encryption and decryption algorithms are similar, if not identical, requiring just a key operation reversal. This drastically reduces the complexity of code or circuitry needed to implement the cipher in software or hardware, respectively (Kessler, 2019). Examples of the Feistel cipher include TWINE (Suzaki et al., 2013), WARP (Banik et al., 2021), DES , RC5 (Rivest, 1995) .

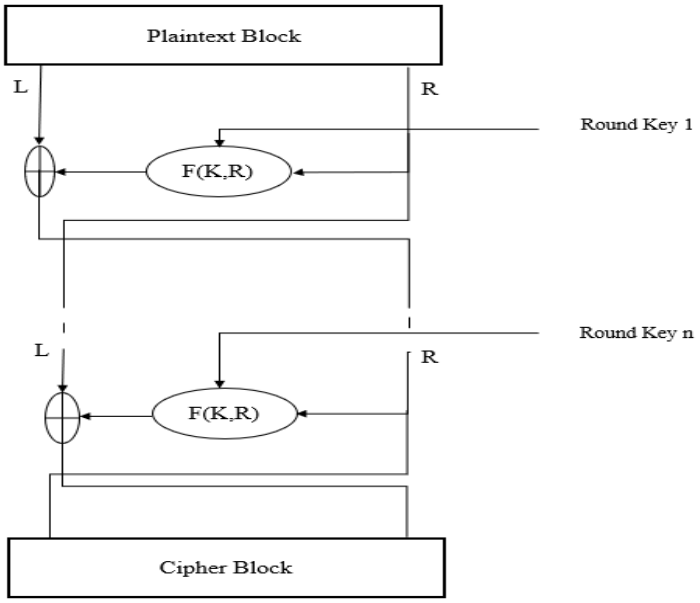

Figure 2.2 Feistel Structure

2.2.3 ARX Structure

Addition-Rotation-Xor, or ARX, is a class of symmetric-key algorithms that only uses modular addition (or bitwise AND operation), bitwise rotation, and exclusive-OR operations (Dinu et al., 2016). The modular addition operation, or bitwise AND, is the source of nonlinearity in ARX-based designs (Beaulieu & Treatman-clark, 2017). The source of non-linear and confusing properties is modular addition, which serves the same purpose as the S-box. Bitwise rotation and bitwise XOR, on the other hand, contribute to the linear mixing and diffusion features (Mohd Esa et al., 2019). Dinu et al., (2016) mentioned that the most efficient software implementation on small processors belonged to ARX ciphers such as SPECK (Beaulieu et al., 2015) which was designed by the American National Security Agency (NSA) in June 2013 and LEA (Hong et al., 2014) by South Korean Electronics and Telecommunications Research Institutes.

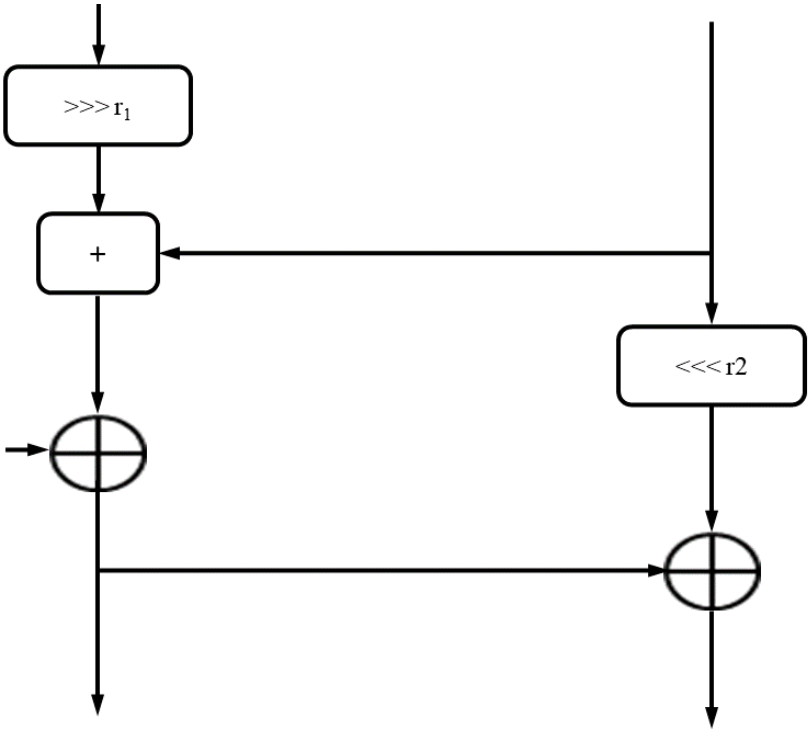

Figure 2.3 SPECK Structure

2.2.4 Sponge Construction

Sponge construction combines a block cipher plus a single permutation in place of compression to create hash function. The sponge function performs an XOR operation to combine the message bits with the internal state rather than utilizing a block cipher (Aumasson, 2017). Absorbing and squeezing are two phases of sponge construction. In absorbing phase, the first chunk of *br* (bitrate), which defines the size of the blocks in which sponge consumes input and return output bits is absorbed through XOR operation and then *f* function is applied to the internal state. After the sponge has absorbed all of the input, then squeezing appends the first *br* bits of the state to the output and *f* function is applied to the internal state. This is repeated until all output has been squeezed out. The state's capacity *c* bits are never used as inputs or modified as the sponge's outputs. The most well-known sponge function is Keccak, also called SHA-3 (Bertoni et al., 2009).

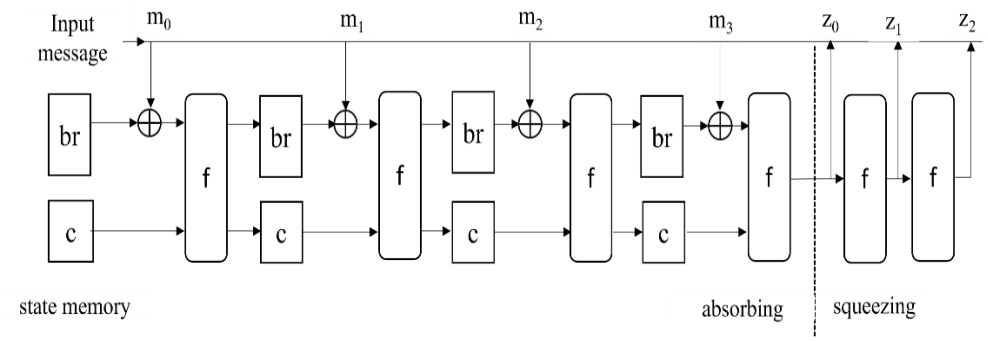

Figure 2.4 Sponge Construction

2.2.5 Davis Meyer Construction

Davies Meyer hash function construction is a simple and efficient method used to construct a cryptographic hash function using a block cipher. The input message *M* is divided into blocks, and each block of the input message is XORed with the current state H_{i-1}, then passed through the block cipher to produce a ciphertext. The ciphertext is then XORed with the current state to update it. This process is repeated for each block, with the final state representing the hash value of the input message. This construction provides a way to create a secure and efficient hash function by iteratively mixing the input message with the hash value using encryption and XOR operations. MD5 and SHA-1 are examples of hash function constructed based on Davis Meyer (Aumasson, 2017).

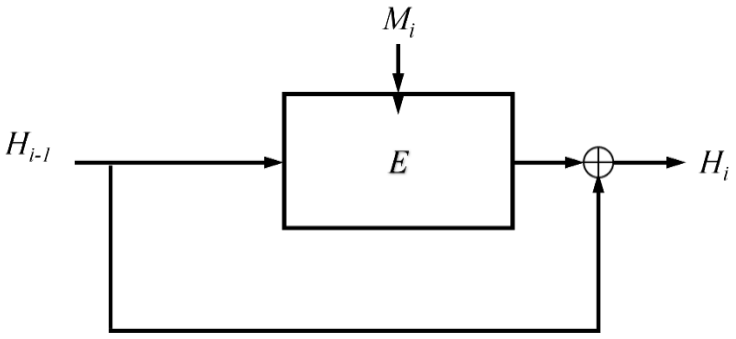

Figure 2.5 Davis-Meyer Construction

2.3 Chaos Theory and Cryptography

Chaos theory is a branch of mathematics that studies nonlinear dynamical systems with the butterfly effect, in which a small change in a system's initial condition can result in large changes in its outputs. A deterministic system that exhibits seemingly random behavior due to its sensitivity to initial conditions is referred to as a chaotic dynamical system. The unpredictable nature of chaotic systems, which resembles noise, has led researchers to study the relationship between cryptography and chaos. As a result, numerous cryptographic algorithms based on chaotic maps have been designed (Ljupco Kocarev, 2001). The properties of chaotic maps, such as sensitivity to changes in initial conditions and control parameters, pseudorandom behaviour, and unstable periodic orbits with long periods, are analogous to the requirements of cryptographic algorithms. The underlying premise of encryption based on chaos is that certain dynamic systems can generate random numerical sequences. These sequences are used to encrypt messages. The system's output appears random to the attacker due to its pseudorandom nature, while it appears as defined to the receiver who knows the parameters to reproduce the random sequence, allowing for decryption. However, while chaotic maps are mainly applicable to real numbers, encryption transformations in cryptography are specified on finite sets. All chaotic maps, however, have parameters that are cryptographically comparable to encryption keys.

There are significant relationships between chaos and cryptography as clearly stated in (Gonzalo Alvarez & Li, 2006), for example, chaotic systems' sensitivity to initial states and system parameters is similar to cryptographic techniques' key and

plaintext sensitivity while mixing properties of chaos is similar to cryptography's diffusion, deterministic dynamics is similar to deterministic pseudo-randomness. This is summarized in Table 2.1.

Table 2.1 Relationship Between Chaotic System and Cryptographic Algorithm (Gonzalo Alvarez & Li, 2006)

Chaotic Property	**Cryptographic Property**	**Description**
Uses a set of real numbers	Finite state of integers	A little change in the input can result in a significant difference in the output.
Iteration	Round	
Parameters	Keys	A little change in the input can result in a significant difference in the output.
Sensitive to initial condition	Diffusion in small changes in key or plaintext.	A small deviation in the input can cause a large change in the output.
Ergodicity	Confusion	For any given input, output has the same distribution.
Mixing property	Diffusion with a small change in one block point to a whole block.	A minor deviation in the local area might have a significant impact on the entire space.
Deterministic dynamic	Deterministic pseudo-randomness.	A deterministic process can produce pseudo-random (random-like) behavior.
Structure complexity	Algorithm complexity	A simple procedure has a high level of complexity.

The use of chaos in cryptography can be attributed to its properties, which are closely related to the cryptographic characteristics of confusion and diffusion (Shannon, 1949). Shannon introduced these ideas considerably earlier than when chaos-based cryptography was first introduced. Additionally, chaotic dynamical systems have the capability to produce pseudorandomness through qualitatively simple systems. A set of features describes the characteristics observed in chaotic systems. The following are the mathematical standards that are used to defined chaos:

- **Trajectory:** The iterative function produces a set of points. The points are in the range of x_0 to xn, where n represents the number of iterations.

- **Initial condition(s):** These are initial input values (which can be one or more) that a chaotic system starts iterating from.

- **Control parameter:** One or more real numbers that is responsible for most of the chaotic behavior.

- **Dynamic instability:** Often known as the butterfly effect, is a characteristic of sensitivity to initial states, where two randomly closed initial conditions follow significantly different and divergent trajectories.

- **Topological mixing:** Shows how the system evolves in time while any defined part of data is constantly transformed with every other specified part.

- **Aperiodicity:** The property whereby a system moves in an orbit that never repeats itself, i.e., these orbits are never periodic.

- **Ergodicity:** Identifies a chaotic trajectory that, irrespective of where it begins, visits all states within dimensional space evenly.

A chaotic attractor is recognized as a stable structure of long-term trajectories within a confined region of phase space. This structure folds the bundle of trajectories back on itself, leading to the mixing and divergence of nearby states (Kavitha & Uma, 2008). This means that a chaotic system can begin with two close initial states and end up with final states that are far apart after some time. An attractor is a set of points in the phase space, which is closely related to the notion of keyspace in cryptography.

Trajectories filled the phase space since every point can serve as an initial condition (Suarez et al., 2016).

For an iterative dynamic system like $X_{n+1} = f(x_n)$, the iterative function describes the output X_{n+1} along with the input x_n . Figure 2.4 shows a chaotic logistic map's iterative function, given an initial value x_0 and control parameter r, where the output of the function serves as the input for the next step. As a result of using the output as an input, this can also be viewed as a feedback system.

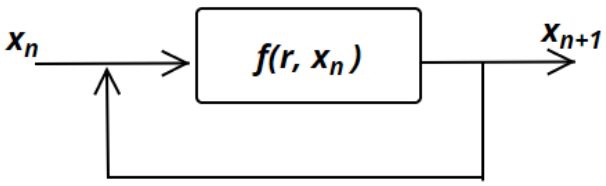

Figure 2.6 Logistic Map Iterating Function

2.4 Chaotic Maps

Chaotic dynamics are common in nature and chaotic behavior can be found in numerous physical systems and mathematical maps. Chaotic maps are iterative functions that, given a set of initial conditions, yield seemingly random results. These initial conditions are often derived from the secret key in chaos-based cryptosystems (Naik & Singh, 2022; Nesa et al., 2019). Chaotic maps can be categorized into discrete and continuous forms. Lorenz map, Chen system among others are examples of well-known continuous-time maps. However, they are not suitable for use in cryptography as compared to discrete maps for the reasons described in Section 2.4.3. The rich dynamics of discrete chaotic maps, as well as the ease with which they may be implemented, makes them suitable for cryptosystem implementation. Short periodic